

Дискреционное разграничение прав в Linux. Основные атрибуты

Андрей Васильев НПИбд-02-19 ¹

12 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

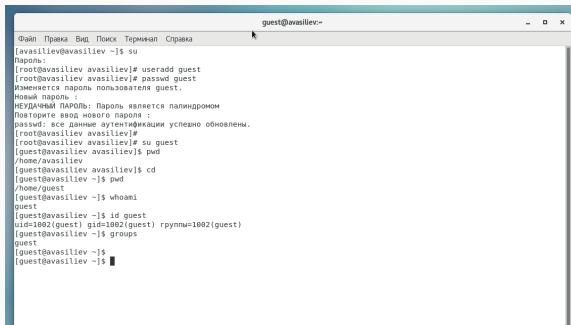
Цели и задачи работы

Цель лабораторной работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Процесс выполнения лабораторной работы

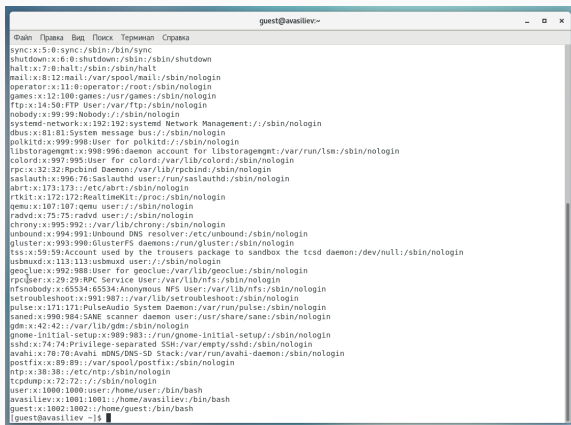
Определяем UID и группу



```
guest@avasiliev:~  
[avasiliev@avasiliev ~]$ su  
Пароль:  
[root@avasiliev avasiliev]# useradd guest  
[root@avasiliev avasiliev]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@avasiliev avasiliev]#  
[root@avasiliev avasiliev]# su guest  
[guest@avasiliev avasiliev]$ pwd  
/home/avasiliev  
[guest@avasiliev avasiliev]$ cd  
[guest@avasiliev ~]$ pwd  
/home/guest  
[guest@avasiliev ~]$ whoami  
guest  
[guest@avasiliev ~]$ id guest  
uid=1002(guest) gid=1002(guest) rгруппы=1002(guest)  
[guest@avasiliev ~]$ groups  
guest  
[guest@avasiliev ~]$  
[guest@avasiliev ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



```
guest@avasiliev:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:8:shutdown:/sbin:/sbin/shutdown  
halt:x:7:8:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:ftp user:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin  
dbus:x:81:81:system message bus:/:/sbin/nologin  
polkitd:x:999:998:User for polkitd:/:/sbin/nologin  
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsn:/sbin/nologin  
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
saslauth:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
abrt:x:173:173:/:etc/abrt:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
gemu:x:107:107:gemu user:/:/sbin/nologin  
radvd:x:175:75:radvd user:/:/sbin/nologin  
chrony:x:995:992:/:var/lib/chrony:/sbin/nologin  
unbound:x:994:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
gluster:x:993:990:GlusterFS daemons:/run/gluster:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:992:988:User for geoclue:/var/lib/geoclue:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:991:987:/:var/lib/setroubleshoot:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saned:x:990:984:SANE scanner daemon user:/usr/share/sane:/sbin/nologin  
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:989:983:/:run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
avahi:x:70:70:avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin  
ntp:x:38:38:/:etc/ntp:/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
user:x:1000:1000:user:/home/user:/bin/bash  
avasiliev:x:1001:1001:/:home/avasiliev:/bin/bash  
guest:x:1002:1002:/:home/guest:/bin/bash  
[guest@avasiliev ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
avasiliiev:x:1001:1001::/home/avasiliiev:/bin/bash
guest:x:1002:1002::/home/guest:/bin/bash
[guest@avasiliiev ~]$ ls -l /home
итого 8
drwx-----, 15 avasiliiev avasiliiev 4096 сен 12 13:07 avasiliiev
drwx-----, 5 guest guest 107 сен 12 13:07 guest
drwx-----, 15 user user 4096 сен 12 11:31 user
[guest@avasiliiev ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/user
lsattr: Отказано в доступе While reading flags on /home/avasiliiev
----- /home/guest
[guest@avasiliiev ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@avasiliev ~]$  
[guest@avasiliev ~]$ cd  
[guest@avasiliev ~]$ mkdir dir1  
[guest@avasiliev ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 12 13:08 dir1  
[guest@avasiliev ~]$ lsattr  
----- ./dir1  
[guest@avasiliev ~]$ chmod 000 dir1  
[guest@avasiliev ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 12 13:08 dir1  
[guest@avasiliev ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@avasiliev ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@avasiliev ~]$
```

Figure 4: Снятие атрибутов с директории

Права и разрешённые действия

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Figure 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.